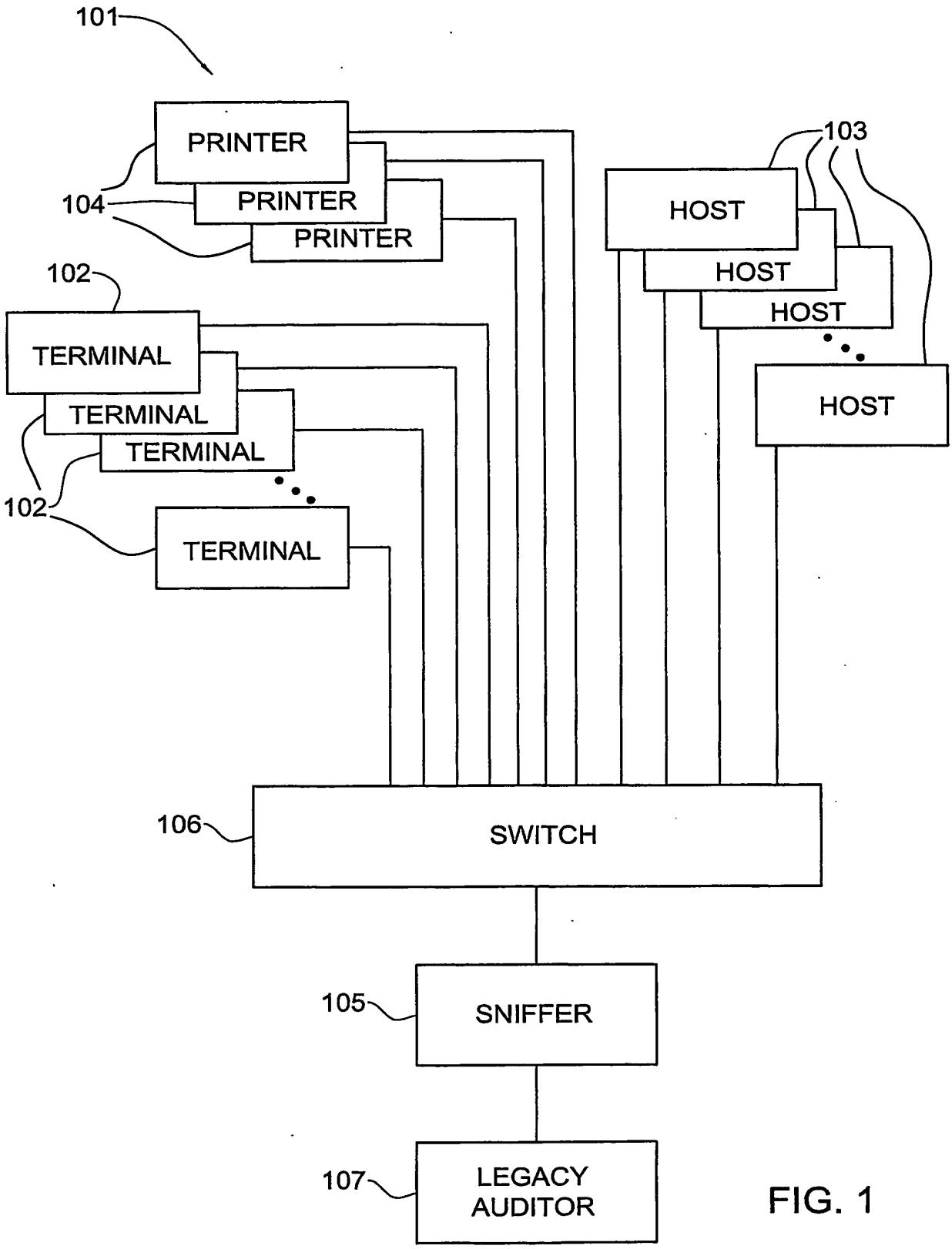
101
PRINTER
PRINTER
PRINTER
104
103
HOST
HOST
HOST
HOST
102
TERMINAL
TERMINAL
TERMINAL
TERMINAL
102
106
SWITCH
105
SNIFFER
107
LEGACY AUDITOR

FIG. 1

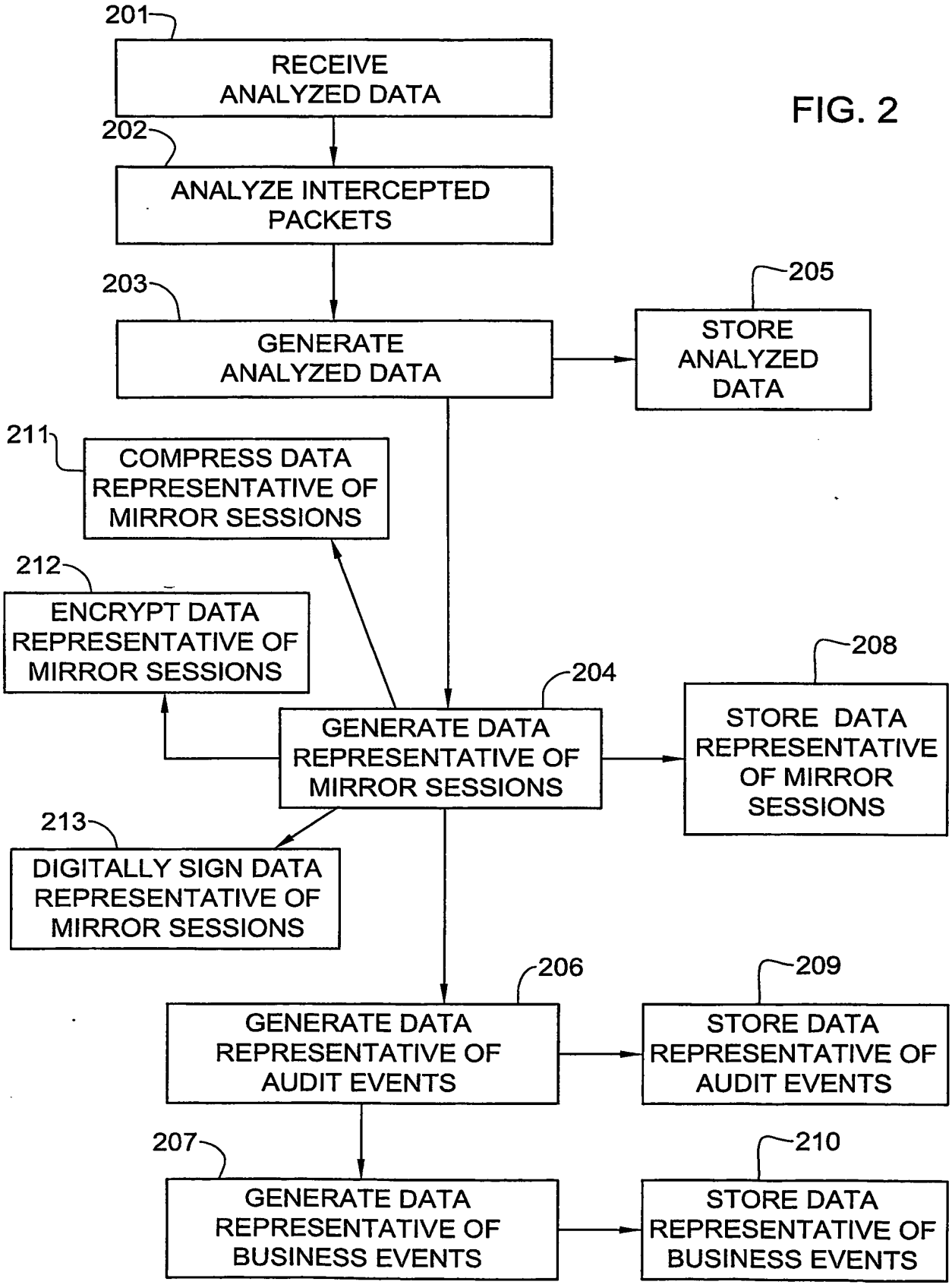
201
RECEIVE ANALYZED DATA
202
ANALYZE INTERCEPTED PACKETS
203
GENERATE ANALYZED DATA
205
STORE ANALYZED DATA
211
COMPRESS DATA REPRESENTATIVE OF MIRROR SESSIONS
212
ENCRYPT DATA REPRESENTATIVE OF MIRROR SESSIONS
204
GENERATE DATA REPRESENTATIVE OF MIRROR SESSIONS
208
STORE DATA REPRESENTATIVE OF MIRROR SESSIONS
213
DIGITALLY SIGN DATA REPRESENTATIVE OF MIRROR SESSIONS
206
GENERATE DATA REPRESENTATIVE OF AUDIT EVENTS
209
STORE DATA REPRESENTATIVE OF AUDIT EVENTS
207
GENERATE DATA REPRESENTATIVE OF BUSINESS EVENTS
210
STORE DATA REPRESENTATIVE OF BUSINESS EVENTS

FIG. 2

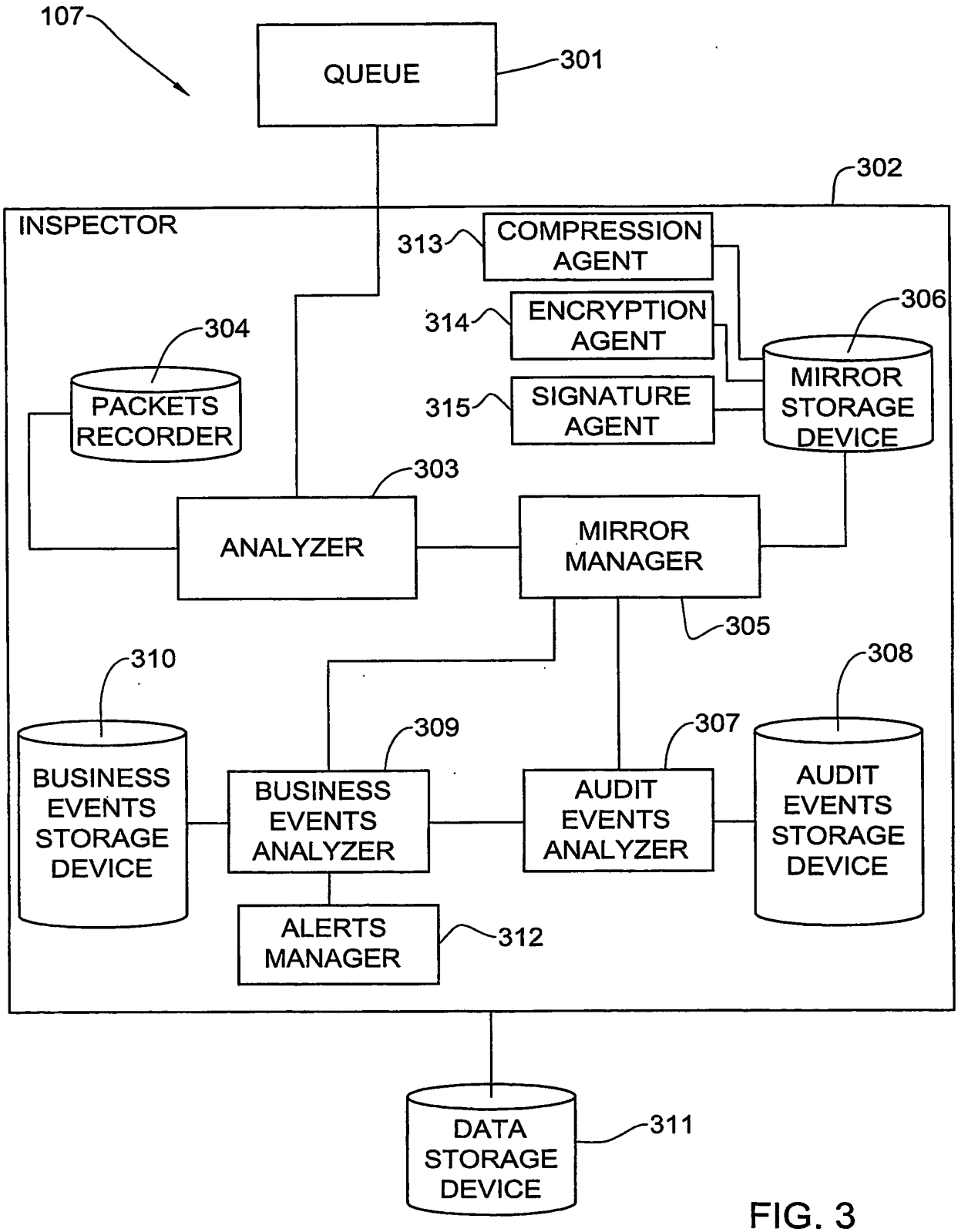
107
QUEUE
301
302
INSPECTOR
313
COMPRESSION AGENT
314
ENCRYPTION AGENT
315
SIGNATURE AGENT
306
MIRROR STORAGE DEVICE
304
PACKETS RECORDER
303
ANALYZER
MIRROR MANAGER
305
310
BUSINESS EVENTS STORAGE DEVICE
309
BUSINESS EVENTS ANALYZER
307
AUDIT EVENTS ANALYZER
308
AUDIT EVENTS STORAGE DEVICE
ALERTS MANAGER
312
DATA STORAGE DEVICE
311

FIG. 3

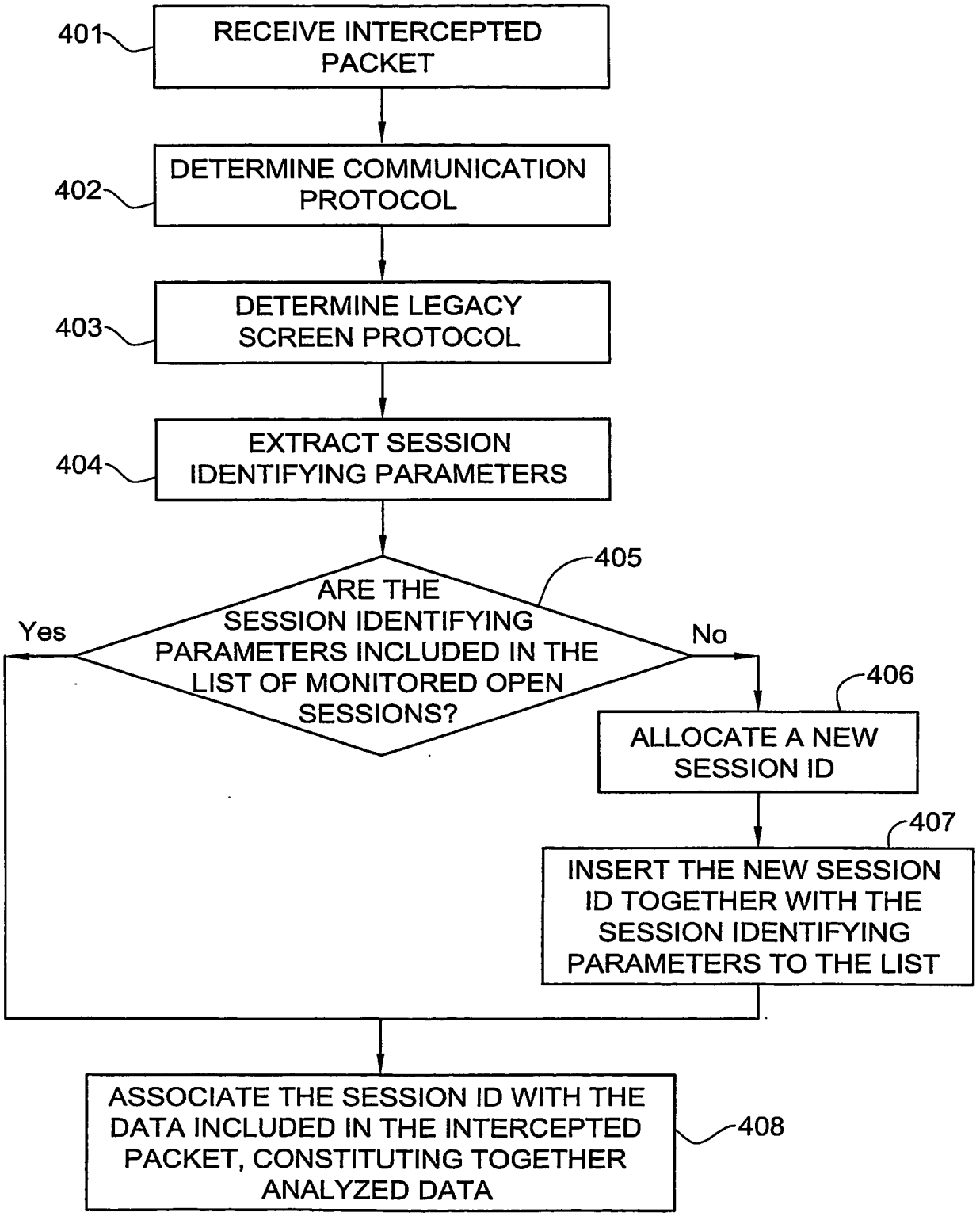
401
RECEIVE INTERCEPTED PACKET
402
DETERMINE COMMUNICATION PROTOCOL
403
DETERMINE LEGACY SCREEN PROTOCOL
404
EXTRACT SESSION IDENTIFYING PARAMETERS
405
ARE THE SESSION IDENTIFYING PARAMETERS INCLUDED IN THE LIST OF MONITORED OPEN SESSIONS?
Yes
No
406
ALLOCATE A NEW SESSION ID
407
INSERT THE NEW SESSION ID TOGETHER WITH THE SESSION IDENTIFYING PARAMETERS TO THE LIST
ASSOCIATE THE SESSION ID WITH THE DATA INCLUDED IN THE INTERCEPTED PACKET, CONSTITUTING TOGETHER ANALYZED DATA
408

FIG. 4

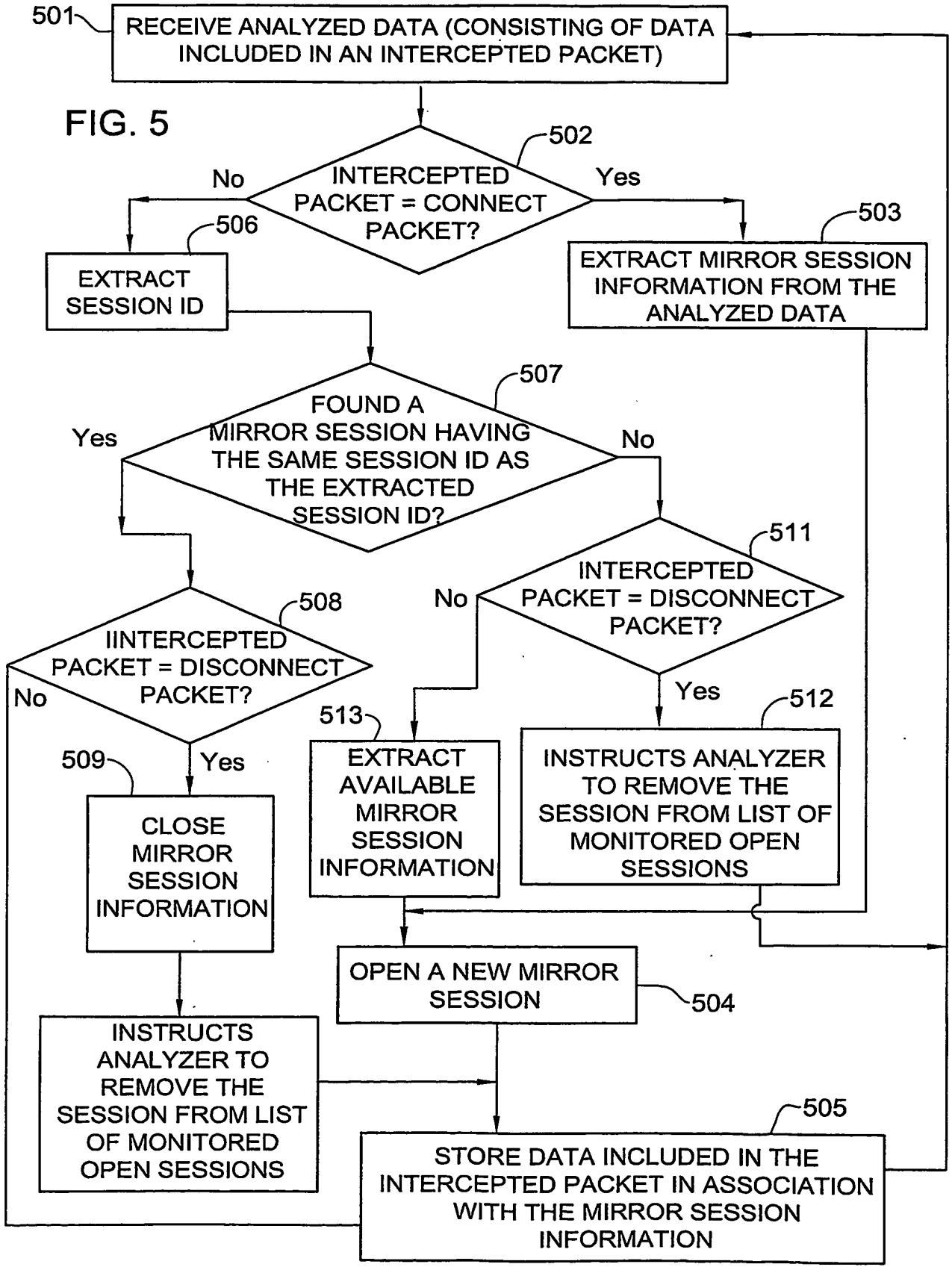
501
RECEIVE ANALYZED DATA (CONSISTING OF DATA INCLUDED IN AN INTERCEPTED PACKET)
502
INTERCEPTED PACKET = CONNECT PACKET?
No
Yes
506
EXTRACT SESSION ID
503
EXTRACT MIRROR SESSION INFORMATION FROM THE ANALYZED DATA
507
FOUND A MIRROR SESSION HAVING THE SAME SESSION ID AS THE EXTRACTED SESSION ID?
Yes
No
508
IINTERCEPTED PACKET = DISCONNECT PACKET?
No
Yes
509
CLOSE MIRROR SESSION INFORMATION
511
INTERCEPTED PACKET = DISCONNECT PACKET?
No
Yes
512
INSTRUCTS ANALYZER TO REMOVE THE SESSION FROM LIST OF MONITORED OPEN SESSIONS
513
EXTRACT AVAILABLE MIRROR SESSION INFORMATION
OPEN A NEW MIRROR SESSION
504
INSTRUCTS ANALYZER TO REMOVE THE SESSION FROM LIST OF MONITORED OPEN SESSIONS
505
STORE DATA INCLUDED IN THE INTERCEPTED PACKET IN ASSOCIATION WITH THE MIRROR SESSION INFORMATION

FIG. 5

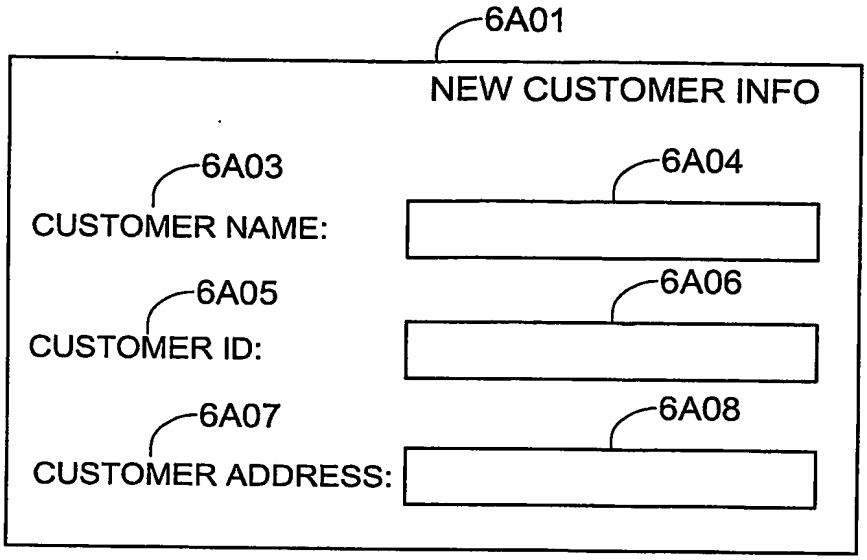
6A01
NEW CUSTOMER INFO
6A03
CUSTOMER NAME:
6A04
6A05
CUSTOMER ID:
6A06
6A07
CUSTOMER ADDRESS:
6A08

FIG. 6A

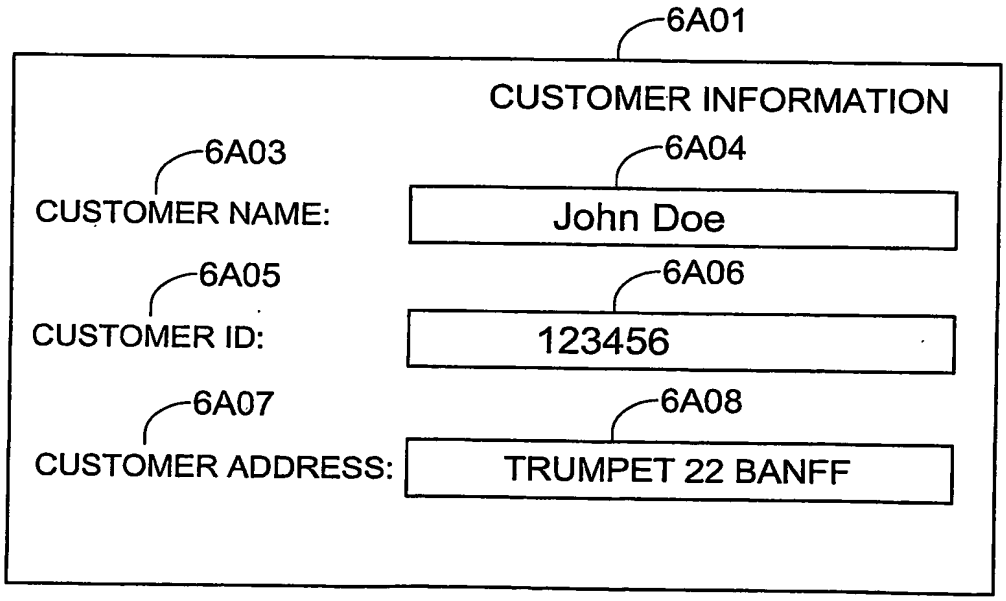
6A01
CUSTOMER INFORMATION
6A03
CUSTOMER NAME:
6A04
John Doe
6A05
CUSTOMER ID:
6A06
123456
6A07
CUSTOMER ADDRESS:
6A08
TRUMPET 22 BANFF

FIG. 6B

6C01

01 C3 11 40	40 1D F0 11	C1 5B 40 D5	C5 E6 40 C3	.C. .0.A$ NEW C
E4 E2 E3 D6	D4 C5 D9 40	C9 D5 C6 D6	D9 D4 C1 E3	USTOMER INFORMAT
C9 D6 D5 11	C3 F1 40 C3	E4 E2 E3 D6	D4 C5 D9 40	ION.C1 CUSTOMER
D5 C1 D4 C5	7A 40 40 40	40 1D 40 11	C4 D8 00 1D	NAME: . .DQ..
F0 11 C5 C1	40 C3 E4 E2	E3 D6 D4 C5	D9 40 C9 C4	0.EA CUSTOMER ID
7A 11 C5 D3	40 1D 50 11	C5 5A 00 1D	F0 11 C6 D1	:.EL .&.E!..0.FJ
40 C3 E4 E2	E3 D6 D4 C5	D9 40 C1 C4	C4 D9 C5 E2	CUSTOMER ADDRES
E2 7A 40 1D	40 11 C7 C2	00 1D F0 11	40 40 40 11	S: . .GB..0. .
C4 C4 13 FF	EF			DD...

FIG. 6C

6D01

7D C6 7B 11	C4 C4 D1 D6	C8 D5 40 C4	D6 C5 11 C5	'F#.DDJOHN DOE.E
D4 F1 F2 F3	F4 F5 F6 11	C6 E4 E3 D9	E4 D4 D7 C5	M123456.FUTRUMPE
E3 40 F2 F2	40 C2 C1 D5	C6 C6 40 40	40 40 40 40	T 22 BANFF
40 FF EF				..

FIG. 6D

6E01

01 C3 11 40	40 1D F0 11	C1 5B 40 D5	C5 E6 40 C3	.C. .0.A$ NEW C
E4 E2 E3 D6	D4 C5 D9 40	C9 D5 C6 D6	D9 D4 C1 E3	USTOMER INFORMAT
C9 D6 D5 11	C3 F1 40 C3	E4 E2 E3 D6	D4 C5 D9 40	ION.C1 CUSTOMER
D5 C1 D4 C5	7A 40 40 40	40 1D 40 D1	D6 C8 D5 40	NAME: . JOHN
C4 D6 C5 11	C4 D8 00 1D	F0 11 C5 C1	40 C3 E4 E2	DOE.DQ..0.EA CUS
E3 D6 D4 C5	D9 40 C9 C4	7A 11 C5 D3	40 1D 50 F1	TOMER ID:.EL .&1
F2 F3 F4 F5	F6 1D F0 11	C6 D1 40 C3	E4 E2 E3 D6	23456.0.FJ CUSTO
D4 C5 D9 40	C1 C4 C4 D9	C5 E2 E2 7A	40 1D 40 E3	MER ADDRESS: . T
D9 E4 D4 D7	C5 D3 C4 D6	D9 40 F2 F2	40 D2 C6 C1	RUMPET 22 BANFF
40 40 40 40	40 40 11 C7	C2 00 1D F0	11 40 40 40	.GB..0.
11 C4 C4 13	FF EF			.DD...

FIG. 6E

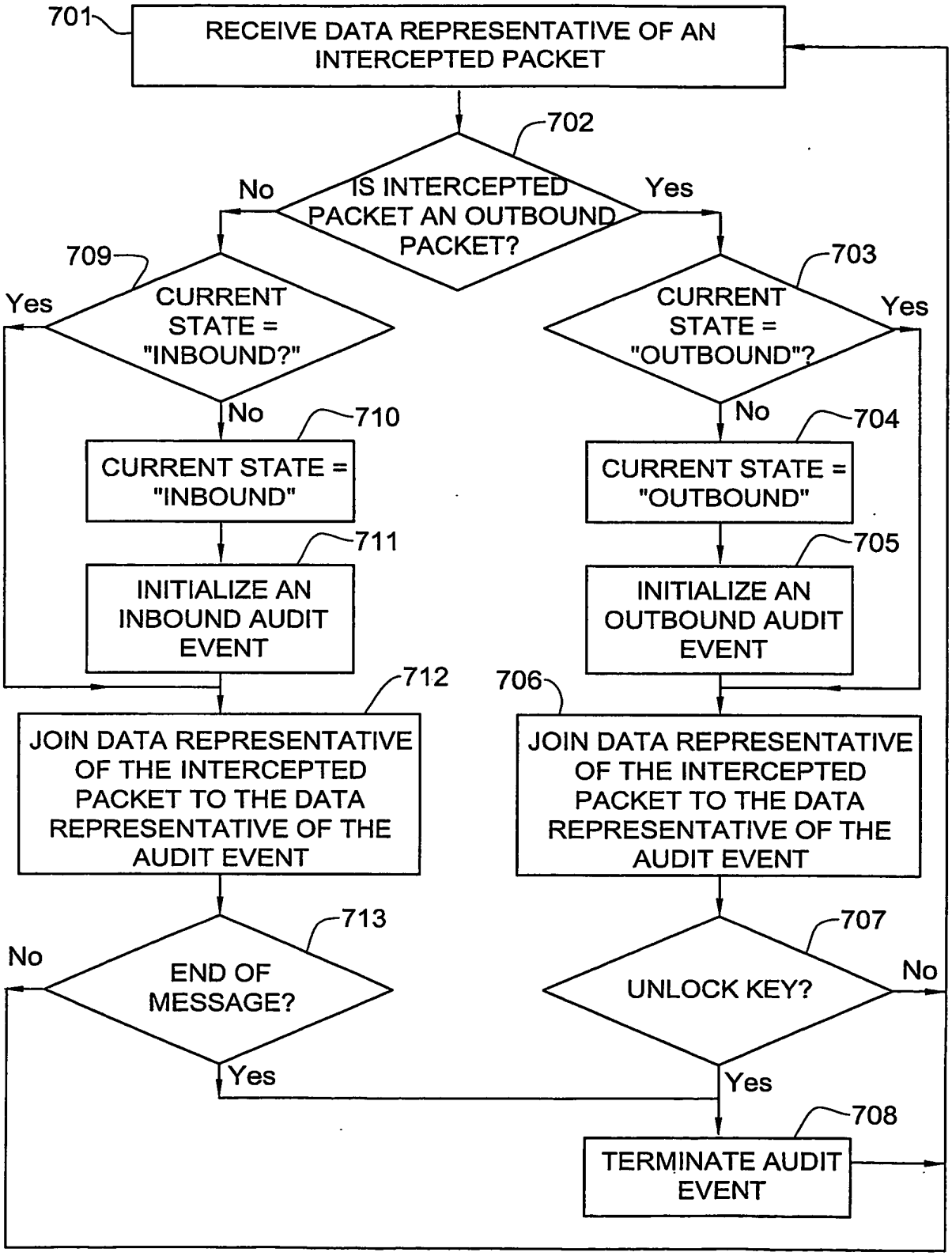
701
RECEIVE DATA REPRESENTATIVE OF AN INTERCEPTED PACKET
702
IS INTERCEPTED PACKET AN OUTBOUND PACKET?
No
Yes
709
CURRENT STATE = "INBOUND?"
Yes
No
710
CURRENT STATE = "INBOUND"
711
INITIALIZE AN INBOUND AUDIT EVENT
703
CURRENT STATE = "OUTBOUND"?
Yes
No
704
CURRENT STATE = "OUTBOUND"
705
INITIALIZE AN OUTBOUND AUDIT EVENT
712
JOIN DATA REPRESENTATIVE OF THE INTERCEPTED PACKET TO THE DATA REPRESENTATIVE OF THE AUDIT EVENT
706
JOIN DATA REPRESENTATIVE OF THE INTERCEPTED PACKET TO THE DATA REPRESENTATIVE OF THE AUDIT EVENT
713
END OF MESSAGE?
No
Yes
707
UNLOCK KEY?
No
Yes
708
TERMINATE AUDIT EVENT

FIG. 7

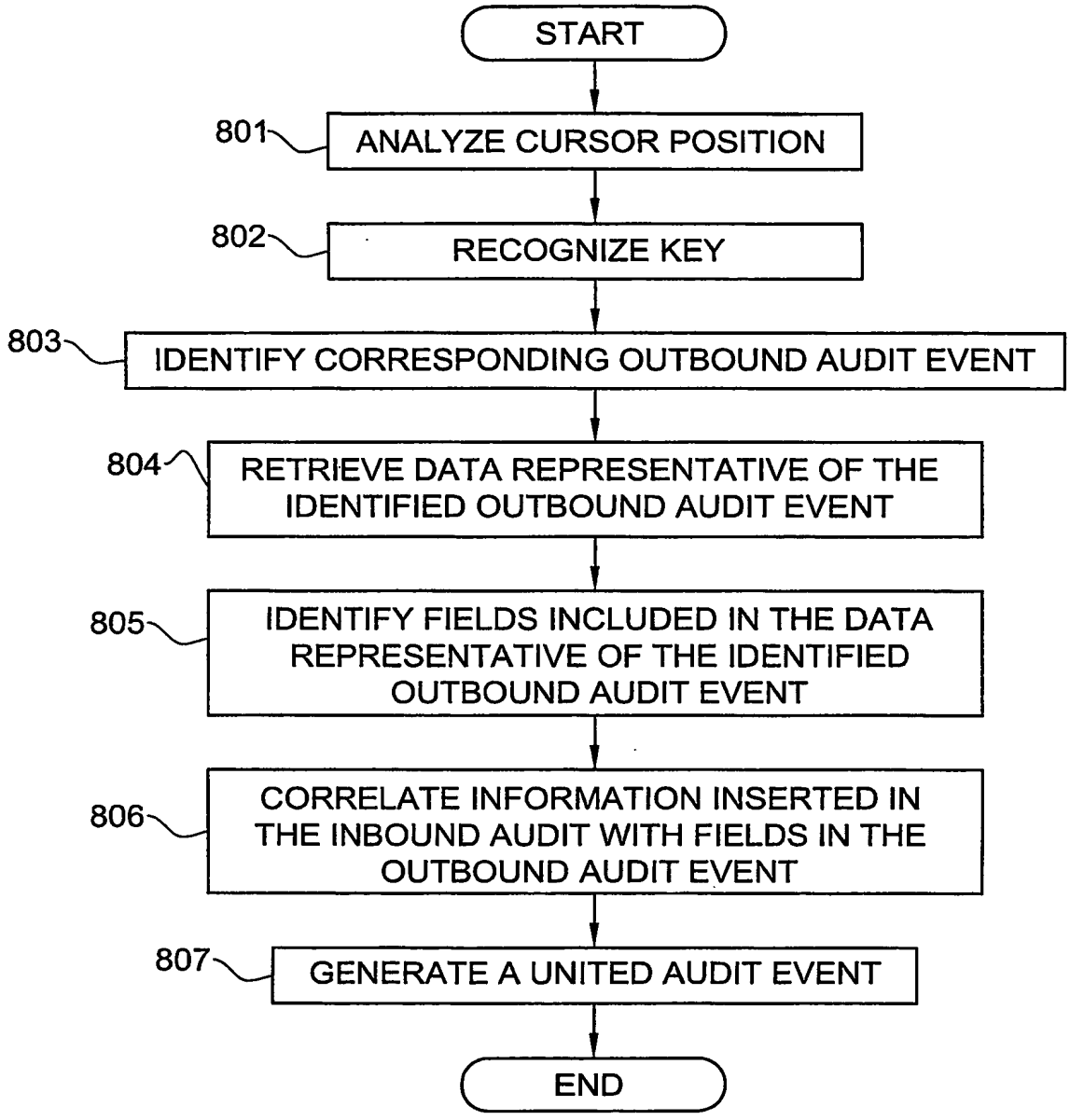
START
801
ANALYZE CURSOR POSITION
802
RECOGNIZE KEY
803
IDENTIFY CORRESPONDING OUTBOUND AUDIT EVENT
804
RETRIEVE DATA REPRESENTATIVE OF THE IDENTIFIED OUTBOUND AUDIT EVENT
805
IDENTIFY FIELDS INCLUDED IN THE DATA REPRESENTATIVE OF THE IDENTIFIED OUTBOUND AUDIT EVENT
806
CORRELATE INFORMATION INSERTED IN THE INBOUND AUDIT WITH FIELDS IN THE OUTBOUND AUDIT EVENT
807
GENERATE A UNITED AUDIT EVENT
END

FIG. 8

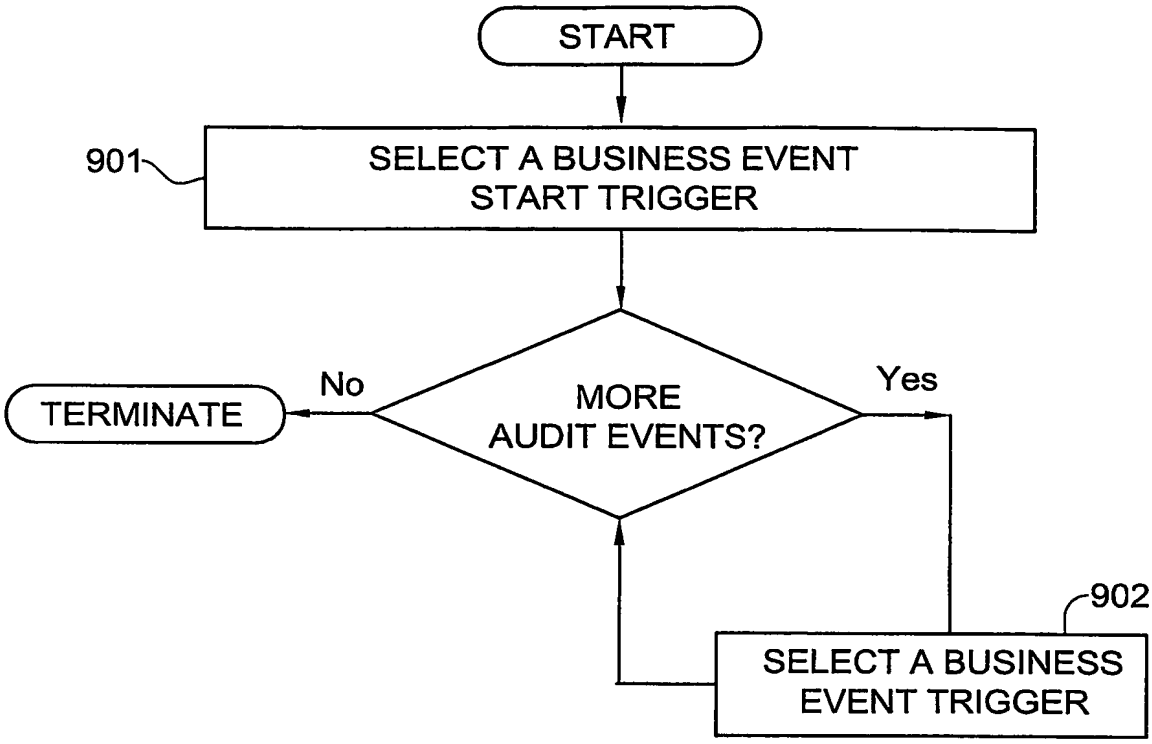
START
901
SELECT A BUSINESS EVENT START TRIGGER
MORE AUDIT EVENTS?
No
TERMINATE
Yes
902
SELECT A BUSINESS EVENT TRIGGER

FIG. 9

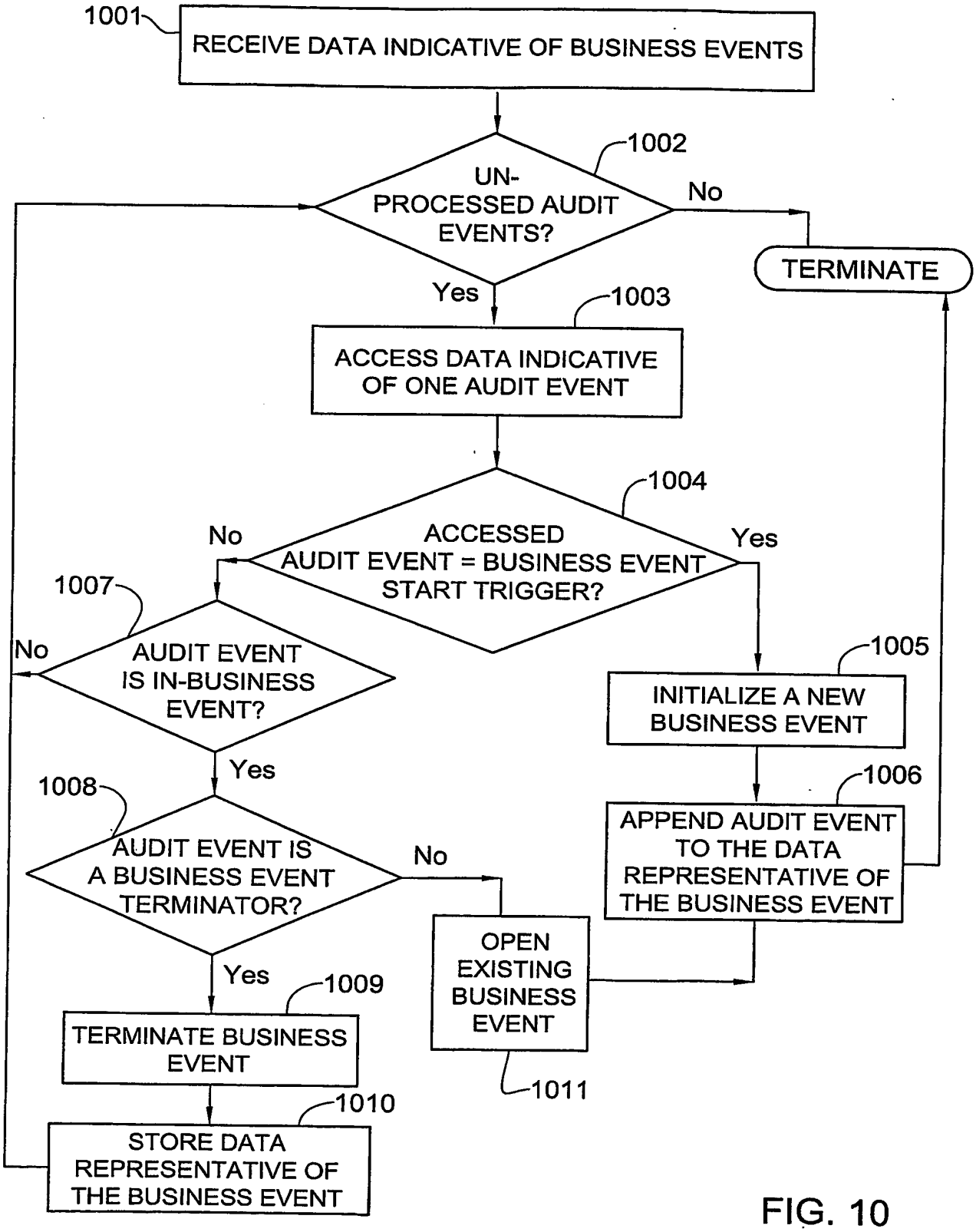
1001
RECEIVE DATA INDICATIVE OF BUSINESS EVENTS
1002
UN-PROCESSED AUDIT EVENTS?
No
TERMINATE
Yes
1003
ACCESS DATA INDICATIVE OF ONE AUDIT EVENT
1004
ACCESSED AUDIT EVENT = BUSINESS EVENT START TRIGGER?
No
Yes
1007
AUDIT EVENT IS IN-BUSINESS EVENT?
No
1005
INITIALIZE A NEW BUSINESS EVENT
Yes
1008
AUDIT EVENT IS A BUSINESS EVENT TERMINATOR?
No
1006
APPEND AUDIT EVENT TO THE DATA REPRESENTATIVE OF THE BUSINESS EVENT
Yes
1009
TERMINATE BUSINESS EVENT
OPEN EXISTING BUSINESS EVENT
1011
1010
STORE DATA REPRESENTATIVE OF THE BUSINESS EVENT

FIG. 10